UNITED STATES BANKRUPTCY COURT
DISTRICT OF NEW JERSEY
Caption in Compliance with D.N.J. LBR 9004-1(b)

BROWN RUDNICK LLP
Robert J. Stark, Esq.
Kenneth J. Aulet, Esq.
Bennett S. Silverberg, Esq.
Susan Sieger-Grimm, Esq.
Seven Times Square
New York, NY 10036
Telephone: (212) 209-4800
Fax: (212) 209-4801
Email: rstark@brownrudnick.com
kaulet@brownrudnick.com
bsilverberg@brownrudnick.com
ssieger-grimm@brownrudnick.com
Proposed Counsel for the Official Committee of Unsecured Creditors
-and-
GENOVA BURNS LLC.
Daniel M. Stolz, Esq.
Donald W. Clarke, Esq.
Gregory S. Kinoian, Esq.
110 Allen Rd., Suite 304
Basking Ridge, NJ 07920
Telephone: (973) 230-2095
Fax: (973) 533-1112
Email: DStolz@genovaburns.com
DClarke@genovaburns.com
GKinoian@genovaburns.com
Proposed Local Counsel for the Official Committee of Unsecured Creditors

BROWN RUDNICK LLP
Stephen D. Palley, Esq.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (617)536-1766
Fax: (617)289-0466
Email: spalley@brownrudnick.com

In re: BLOCKFI INC., *et al.*, Debtors.[1]	Chapter 11 Case No. 22-19361 (MBK) Jointly Administered

[1] The Debtors in these Chapter 11 cases, along with the last four digits of each Debtor's federal tax identification number, are: BlockFi Inc. (0015); BlockFi Trading LLC. (2487); BlockFi Lending LLC (5017); BlockFi Wallet LLC (3231); BlockFi Ventures LLC (9937); BlockFi International Ltd. (N/A); BlockFi Investment Products LLC (2422); BlockFi Services, Inc. (5965) and BlockFi Lending II LLC (0154). The location of the Debtors' service address is 201 Montgomery Street, Suite 263, Jersey City, NJ 07302.

DECLARATION OF MAXWELL GALKA IN SUPPORT OF THE JOINDER OF THE OFFICIAL COMMITTEE OF UNSECURED CREDITORS TO DEBTORS' MOTION FOR ENTRY OF AN ORDER (I) AUTHORIZING THE DEBTORS TO FILE A CONSOLIDATED LIST OF TOP 50 UNSECURED CREDITORS AND CONSOLIDATED LIST OF CREDITORS, (II) AUTHORIZING THE DEBTORS TO REDACT CERTAIN PERSONALLY IDENTIFIABLE INFORMATION OF INDIVIDUAL CREDITORS, CLIENTS, EQUITY HOLDERS, AND CURRENT AND FORMER EMPLOYEES, (III) AUTHORIZING CLIENT NAME REDACTION, (IV) WAIVING THE REQUIREMENT TO FILE AN EQUITY LIST AND PROVIDE NOTICES DIRECTLY TO EQUITY SECURITY HOLDERS, AND (V) GRANTING RELATED RELIEF.

I, MAXWELL GALKA, hereby declare under penalty of perjury, as follows:

1. I am the founder and chief executive officer of Elementus, Inc., a blockchain intelligence and forensics company based in New York, New York, and a proposed forensics advisor to the Official Committee of Unsecured Creditors (the "**Committee**") of the above-captioned Debtors.

2. I submit this declaration (the "**Declaration**") in support of the *Joinder of the Official Committee of Unsecured Creditors to the Debtors' Motion for Entry of an Order (I) Authorizing the Debtors to File a Consolidation List of Top 50 Unsecured Creditors and Consolidated List of Creditors, (II) Authorizing the Debtors to Redact Certain Personally Identifiable Information of Individual Creditors, Clients, Equity Holders, and Current and Former Employees, (III) Authorizing Client Name Redaction, (IV) Waiving the Requirement to File an Equity List and Provide Notices Directly to Equity Security Holders, and (V) Granting Related Relief*, (the "**Joinder**") filed contemporaneously herewith, and (b) the *Debtors' Motion for Entry of an Order (I) Authorizing the Debtors to File a Consolidation List of Top 50 Unsecured Creditors and Consolidated List of Creditors, (II) Authorizing the Debtors to Redact Certain Personally Identifiable Information of Individual Creditors, Clients, Equity Holders, and Current and Former Employees, (III) Authorizing Client Name Redaction, (IV) Waiving the Requirement to File an*

Equity List and Provide Notices Directly to Equity Security Holders, and (V) Granting Related Relief [Docket No. 4] (the "**Consolidation and Redaction Motion**").[2] I am over 18 years old and authorized to submit this Declaration on behalf of the Committee.

3. I hold degrees in finance and computer science engineering from the University of Pennsylvania. I have also served as an adjunct lecturer in data science at the University of Pennsylvania. I have over 15 years of data science, finance, and quantitative analysis experience, including experience trading complex derivatives at global investment banks.

4. I specialize in blockchain intelligence and forensics analysis, including investigating complex transactions and flow of funds activities that occur on blockchains. I also specialize in analyses that monitor and trace illicit activity and ransomware attacks that are often designed to be hidden on blockchains. My analyses are often performed to help protect individuals and businesses from risks associated with blockchains and cryptocurrencies.

5. In particular, I have substantial experience assisting federal law enforcement in investigating thefts of cryptocurrency and other crimes in which cryptocurrency was used to facilitate unlawful activities. A core part of my business as chief executive officer of Elementus is to find addresses onchain that belong to malefactors. I also advise cryptocurrency service providers on ways to avoid contact with suspected malefactors who might be engaged in money laundering or other unlawful activities. Based upon this work, I have become familiar with the methods and tactics malefactors commonly use to target businesses and individuals.

6. The statements in this Declaration are, except where noted specifically, based on my personal knowledge or on information that I have received from either the Committee or employees of Elementus working directly with me or under my supervision, direction, or control.

---

[2] Capitalized terms used but not defined herein have the meanings ascribed to them in the Joinder.

Neither Elementus nor I am being compensated specifically for this testimony other than compensation to Elementus as a professional services firm proposed to be retained by the Committee. If I were called upon to testify, I could and would competently testify to the facts set forth herein on that basis.

A. Public Disclosure of Personally Identifiable Information Creates a Risk of Unlawful Injury to Account Holders and Their Cryptocurrency.

7. In my experience, malefactors target known cryptocurrency holders. A malefactor will know that a person holds cryptocurrency if his or her personally identifiable information is disclosed in these cases. It becomes substantially easier for malefactors to target cryptocurrency holders if the malefactors possess those holders' personally identifiable information. I understand that the Debtors' statements of financial affairs and schedules of assets and liabilities, the creditor matrix, and other documents to be filed in these Chapter 11 cases will contain personally identifiable information, including (a) names, (b) physical addresses, (c) mailing addresses, or (d) email addresses (collectively, "**PII**"), if the Consolidation and Redaction Motion is not granted. The schedules of assets and liabilities is of particular concern because it lists individual account holders and their respective cryptocurrency holdings, thus identifying account holders who hold relatively larger amounts of cryptocurrency for malefactors. However, any release of account holder PII poses significant risks. Every commonly used scheme to steal cryptocurrency (whether in hot wallets or hardware wallets) will be easier to perform if malefactors know the PII of people who hold cryptocurrency. Some of the main risks to account holders are described below.

8. **Phishing Attacks.** There are multiple types of phishing attacks. One type occurs when an account holder receives a message (either via email, instant message, or text message) from an attacker masquerading as a trusted entity. An unsuspecting account holder may willingly provide sensitive information directly to the malefactor if he or she believes that a fraudulent email

is from a trusted source. Alternatively, an account holder may indirectly provide such information and access by clicking on a link in an email, instant message, or text message received from a malefactor that causes a computer program (a "**Trojan**") to infect that holder's target device. The Trojan can then send sensitive information from the targeted account holders' infected device to the malefactor. Additionally, an attack that is becoming increasingly common involves a malefactor pretending to be someone with whom the account holder has a relationship and using that appearance of a relationship to exploit the holder into providing sensitive information. From my experience, I know that these different phishing attacks have been used to obtain private keys and account credentials to steal cryptocurrency.

9. What all of these "phishing" attacks have in common is that, in order to succeed, they must appear authentic. A fraudulent source can appear legitimate with the inclusion of the trusted source's logo/trademark, color scheme, or typography. However, one of the most reliable means of feigning legitimacy is to include the particular account holder's PII in the message, which adds a veil of authenticity and credibility to the fraudulent communication. This makes the release of account holders' PII (which most account holders will not even be aware has occurred) particularly dangerous.

10. **Account Spoofing.** Spoofing is when a malefactor disguises an email address, display name, phone number, text message, or website URL to convince an account holder that he or she is interacting with a trusted source. As an example, a malefactor might write an account holder in these cases from an email address that appears to be from a trusted source but is actually from a fake domain name with a subtle aberration like "@blcokfi.com" (in which the "o" and "c" have been switched) or "@blockfi.net" (rather than ".com"). An account holder is less likely to be suspicious of these emails—and thus less likely to notice the minor errors in domain names that

might alert them to the fraud—if the emails contain the account holder's PII, which the account holder perceives as indicia of authenticity. I know from experience that a malefactor will more easily be able to steal private keys or cryptocurrency from wallets once he or she has obtained the necessary information from the account holder.

11. **SIM Swapping.** Another risk to account holders if PII is disclosed is "SIM swapping," which is when a malefactor gains access to an account holder's account vis-à-vis the holder's cellphone through an accomplice at a wireless provider. That provider will issue a new SIM card for the account holder's phone to the malefactor so the malefactor can take over the holder's number on a new device with the new SIM. Most providers of online wallets rely on text messaging for resetting passwords or perform two-step multifactor authentication to gain access to the wallets or private keys. A malefactor who has obtained a SIM swapped device can effortlessly authenticate and obtain access to the contents of the phone belonging to the targeted account holder, including private keys and other sensitive information.

12. **Real Life Threats.** In addition to these virtual threats, if account holders' PII is disclosed, they may be vulnerable to real-life threats, including robberies and other threats of violence. I am aware of various incidents in which holders of cryptocurrency have been robbed at gun point, being forced to surrender private keys, passwords, and other access credentials to online wallets.

B. There is Still a Risk of Harm to Account Holders if Only Their Names are Made Public.

13. The types of attacks described above can occur even if only names are disclosed. I know from my experience that merely the name of an individual who holds cryptocurrency is enough for a malefactor to obtain additional information about that individual from data that has been aggregated from hacks of other cryptocurrency companies, such as Coinbase and Kraken.

This account holder data is available on the so-called "dark web." The dark web is a part of the internet that contains encrypted content that is accessible with only a special software or browser. Those with access to the dark web can remain anonymous and untraceable, allowing malefactors to engage in illegal activities with impunity. I also know from experience that a malefactor could run an account holder name through a "people search" on the internet to obtain more information in an effort to steal the account holder's cryptocurrency holdings. A people search is a query function on a website that is not on the dark web and is accessible upon paying a small fee. I have personal knowledge of account holders who have been victims of cryptocurrency theft or other cryptocurrency crimes after their information was obtained on the dark web or via people searches.

14. In addition, cryptocurrency is an intangible bearer instrument and must be stored by the owner in a wallet or on a platform. I know that cryptocurrency holders typically store their cryptocurrency in more than one wallet or use multiple online platforms. This is the case because, among other things, (a) certain wallets are only capable of storing certain types of cryptocurrency and cryptocurrency holders typically have more than one type of currency, (b) cryptocurrency companies vary as to what types of cryptocurrency transactions can be performed on their platforms, and (c) cryptocurrency companies differ in the services they offer account holders. A malefactor who knows the names of people in these cases can reasonably expect that they have other wallets or use other platforms that are unaffiliated with the Debtors (*e.g.*, Coinbase, FTX, Gemini, etc.). Thus, the public disclosure of names makes cryptocurrency stored elsewhere a target.

15. I know from experience that having the name of a person who holds cryptocurrency is enough to subject him or her to phishing, account spoofing, physical attacks, and other unlawful injury. This risk of unlawful injury is also material if either addresses or email addresses are

disclosed. Cryptocurrency is an attractive target for malefactors because it is easy to liquidate and transactions are anonymous. Once someone's cryptocurrency is stolen, it is near impossible to recover those assets or find the perpetrator. I, therefore, believe this it is prudent to safeguard account holders' names and other PII in the first instance rather than seek to remedy the deleterious effects of a crime should one occur as a result of PII being publicly disclosed—a disclosure to which the Debtors' account holders have not consented and are likely not aware.

Dated: January 10, 2023
New York, New York

Respectfully submitted,

/s/ Max Galka

Name: Max Galka
Title: Founder and Chief Executive Officer
Elementus Inc.